Day : Wednesday

PALM INTRANET

Date: 6/21/2006
Time: 17:49:58

Inventor Name Search Result

Your Search was:

Last Name = ISHIKAWA
First Name = MARK

Application#	Patent#	Status	Date Filed	Title	Inventor Name
09670242	Not Issued	41	09/26/2000	Method, apparatus, and system for managing, reviewing, comparing and detecting data on a wide area network	ISHIKAWA, MARK M.
09821259	Not Issued	61	03/29/2001	System, method and apparatus for authenticating the distribution of data	ISHIKAWA, MARK M.
09821565	Not Issued	71	03/29/2001	System, method and apparatus for preventing transmission of data on a network	ISHIKAWA, MARK M.
10845436	Not Issued	30	05/12/2004	Identification and tracking of digital content distributors on wide area networks	ISHIKAWA, MARK M.
11096554	Not Issued	30	04/01/2005	Method and apparatus for detecting email fraud	ISHIKAWA, MARK M.
11103821	Not Issued	20	04/11/2005	Identification and tracking of digital content distributors on wide area networks	ISHIKAWA, MARK M.
11396233	Not Issued	19	03/31/2006	System and method for distributing and tracking media	ISHIKAWA, MARK M.
60193653	Not Issued	159	03/30/2000	System, method and apparatus for authenticating the distribution of advertisements	ISHIKAWA, MARK M.
60193654	Not Issued	159	03/30/2000	System, method and apparatus for preventing transmission of data on a network	ISHIKAWA, MARK M.
60200054	Not Issued	159	04/27/2000	System, method and apparatus for preventing transmission of data on a network	ISHIKAWA, MARK M.
60215780	Not Issued	159	07/05/2000	Method apparatus and system for managing controlling access and filtering of content and data on a computer system	ISHIKAWA, MARK M.

60667721	Not Issued	159	04/01/2005	System and method for distributing and tracking media	ISHIKAWA, MARK M.

Inventor Search Completed: No Records to Display.

Search Another: Inventor

Last Name ISHIKAWA **First Name** MARK Search

To go back use Back button on your browser toolbar.

Back to PALM | ASSIGNMENT | OASIS | Home page

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	207	shar$4 near10 (security or attack$4 or intru$4) near10 (switch$4 or router$1 or peer$3 or neighbor$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 12:55
L2	78	l1 and @ad<"20020101"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 12:55
L3	4	shar$4 near10 (security or attack$4 or intru$4) near10 (switch$4 or router$1 or peer$3 or neighbor$4) with address$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 13:06
L4	12377	370/389,392,401,390,432.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 13:07
L5	81	l4 and (send or sent or alert$3 or alarm$3 or shar$3 or stop$3 or inhibit$4 or prohibit$4) with (security or intru$4 or attack$4) with (switch$4 or rout$4 or peer$3 or neighbor$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 13:21
L6	81	l5 and ad<"20020101"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 13:09
L7	1291	370/390,432.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 13:24
L8	8436	"726"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 13:21

EAST Search History

L9	26066	"713"/$.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 13:21
L10	1	l7 and l8 and l9	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 13:22
L11	283	l7 and (broadcast or anounc$4) with address$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 13:26
L12	196	l11 and @ad<"20020101"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 13:25
L13	12	l7 and (broadcast or anounc$4) with address$3 with (alert$3 or alarm$4 or shar$4 or stop$4 or ceas$4 or inhibit$4 or prohibit$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 14:17
L14	2	"20030167404".pn.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 14:35
L15	2074	726/3,22,11,12,13,14,23.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 14:53
L16	184	713/163.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 14:54

EAST Search History

L17	33	l16 and (broadcast or announc$4) with address$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 14:58
L18	16	l17 and @ad<"20000301"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 15:04
L19	0	l16 and (broadcast or announc$4) with (inhibit or stop$4 or prohibit$4 or ceas$4 or prevent$4) with address$3	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 14:58
L20	5127	709/238	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 15:31
L21	2580	709/238.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 15:31
L22	0	l21 and (stop$4 or ceas$4 or inhibit$4 or prohibit$4 or prevent$4 or alert$3 or alarm$3 or shar$4) with (security or attack$4 or intru$4) with address$3 with (announc$4 or releas$4 or broadcast$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 15:34
L23	4	(l7 or l8 or l9) and (stop$4 or ceas$4 or inhibit$4 or prohibit$4 or prevent$4 or alert$3 or alarm$3 or shar$4) with (security or attack$4 or intru$4) with address$3 with (announc$4 or releas$4 or broadcast$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 15:34
S1	12	(ceas$4 or alarm or alert or inhibit$4 or prohibit$4 or stop$3) near4 (anounce$4 or transmis$4 or provid$4) near4 address$2 near10 (firewall or server or router$1 or switch$3)	USPAT	OR	OFF	2006/06/21 10:40

EAST Search History

S2	13	(ceas$4 or alarm or alert or inhibit$4 or prohibit$4 or stop$3) near4 (anounce$4 or transmis$4 or provid$4 or broadcast$4) near4 address$2 near10 (firewall or server or router$1 or switch$3)	USPAT	OR	OFF	2006/06/21 10:55
S3	1	"5625886".PN.	USPAT; USOCR	OR	OFF	2006/06/21 10:45
S4	1	"4939746".PN.	USPAT; USOCR	OR	OFF	2006/06/21 10:47
S5	40	(ceas$4 or alarm or alert or inhibit$4 or prohibit$4 or stop$3) near4 (anounce$4 or transmis$4 or provid$4 or broadcast$4) near4 address$2 near10 (firewall or server or router$1 or switch$3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 10:56
S6	15	S5 and @ad<"20020101"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 12:53

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L24	486	709/242.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 15:51
L25	0	l24 and (stop$4 or ceas$4 or inhibit$4 or prohibit$4 or prevent$4 or alert$3 or alarm$3 or shar$4) with (security or attack$4 or intru$4) with address$3 with (announc$4 or releas$4 or broadcast$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 15:51

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	366	726/23.ccls.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 17:39
L2	77187	Ishikawa.in.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 17:40
L3	85	l2 and rout$4 with address$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 17:40
L4	12	l3 and (broadcast or announc$4 or inhibit$4 or prohibit$4 or stop$4 or ceas$4 or prevent$4 or alert$4 or alarm$4) with address$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 17:43
L5	3	l3 and (arbitor$4 or router$1 or switch$4 or firewall or traffic) with (attack$4 or security or intru$4)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 17:44
L6	37	l3 and (arbitor$4 or router$1 or switch$4 or firewall or traffic) with address$4	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/06/21 17:45

```
Set     Items   Description
S1     208989   S ATTACK? OR ANOMAL? OR ABNORMAL?
S2     162269   S OVERFLOW? OR FLOOD? OR SYNFLOOD? OR VIRUS? OR WORM? ? OR TROJAN()HORSE?
OR MALWARE? OR MALICIOUS()CODE?
S3      23144   S DENIAL?(2W)SERVICE? OR INTRUSION? OR MALICIOUS? OR HOSTILE? OR
OVERWHELM? OR SWAMP?
S4     277722   S SUSPICIOUS? OR (ABNORM? OR ANOMAL?)(2N)ACTIVIT? OR HACK? OR PENETRAT? OR
ATTACK? OR VIOLAT? OR UNAUTHORI?
S5    2514425   S MONITOR? OR TRANSDUCE? OR TRANSDUCING? OR SENSING? OR DETECT? ? OR
DETECTION? OR DETECTED OR DETECTING
S6    1338414   S TRACK? OR AUDIT? OR POLL? OR INTERROGAT? OR PING? OR TEST? OR SURVEY?
S7    1688748   S SURVEILL? OR INSPECT? OR QUIZ? OR EVALUAT? OR ASSESS? OR ASCERTAIN? OR
MEASUR?
S8    1561527   S IDENTIF? OR DISCOVER? OR FIND? OR LOCAT? OR PINPOINT? OR SPOT? ? OR
SPOTTING? OR SPOTTED
S9     713229   S RECOGN? OR PERCEIV? OR DISCERN? OR EXPOSE? OR EXPOSING OR FERRET? OR
UNCOVER?
S10    119938   S S1:S4(10N)S5:S9
S11     27414   S INHIBIT? OR STOP? OR TERMINAT? OR END OR ENDS OR ENDED OR ENDING?
S12       629   S CEASE? OR CEASING OR CESSATION? OR ARREST? OR SHUT?()DOWN?
S13      1889   S SHUT?()DOWN? OR SHUTDOWN? OR DISABL? OR DISCONTINU? OR DEACTIVAT? OR
HALT?
S14      2552   S "NOT" ()ENABL? OR SUSPEND? OR SUSPENSION? OR CANCEL?
S15      6909   S AUTODISABL? OR NOGO OR NO()GO OR OFFSTATE? OR OFF()STATE? OR INTERRUPT?
OR TURNOFF? OR (TURN? OR SWITCH? OR SHUT?)()OFF
S16     25285   S ROUTE? OR ROUTING? OR SEND? OR BROADCAST? OR TRANSMIT? OR TRANSMISSION?
S17      8137   S FORWARD? OR DISEMINAT? OR DISSEMINAT? OR DISPATCH? OR FORWARD? OR
TRANSLOCAT? OR TRANSPORT?
S18      9042   S ADDRESS? OR RETURNADDRESS? OR LOCATION? OR LOCALE? OR LOCALIT? OR SITE?
? OR WEBADDRESS? OR URL OR URLADDRESS?
S19      5148   S REGION? ? OR SECTOR? ? OR MACADDRESS? OR IPADDRESS? OR NAT? ? OR
WEBSITE?
S20         7   S (WEB OR WORLD()WIDE()WEB OR ONLINE OR INTERNET OR LAN? ? OR WAN? ?)()(ID
OR IDENTIF? OR IDS)
S21     14474   S ROUTER? OR SWITCH?
S22       777   S (ROUTING OR SWITCHING)()(DEVICE? OR UNIT? OR APPARATUS? OR FIREWALL? OR
PROXY? OR SERVER?)
S23       402   S (ROUTING OR SWITCHING)()(UNIT? OR MODULE? OR COMPONENT? OR HARDWARE? OR
HUB? ? OR NODE?)
S24      5779   S NETWORK? OR LAN OR WAN OR LANS OR WANS OR ETHERNET? OR INTRANET? OR
EXTRANET? OR VPN? ?
S25      1648   S WEB OR (COMMUNICAT? OR TELECOM? OR TELCOM? OR TELNET?)()SYSTEM?
S26     13994   S IC=G06F?
S27     11858   S MC=T01?
S28     34594   S S10 AND S20:S27
S29        36   S S28 AND S11:S15(6N)S16:S17(6N)S18:S20
S30        66   S S10 AND S11:S15(5N)S16:S17(5N)S18:S20
S31        52   S S30 AND S1:S4(5N)S5:S9
S32        73   S S29:S31
S33        16   S S32 AND AC=US/PR
S34        13   S S33 AND AY=(1970:2000)/PR
S35        12   S S33 NOT AY=(2001:2006)/PR
S36        57   S S32 NOT S33
S37        37   S S36 AND PY=1970:2000
S38        36   S S36 NOT PY=2001:2006
S39        50   S S34:S35 OR S37:S38
S40        50   IDPAT (sorted in duplicate/non-duplicate order)
 ; show files
```

[File 347] **JAPIO** Dec 1976-2005/Dec(Updated 060404)

[File 350] **Derwent WPIX** 1963-2006/UD,UM &UP=200639

**File 350: Preview the enhanced DWPI through ONTAP DWPI (File 280). For more information, visit http://www.dialog.com/dwpi/.*

40/3,K/12 (Item 12 from file: 350) **Links**
Derwent WPIX

010744066 **Image available**
WPI Acc No: 1996-241021/199625
XRPX Acc No: N96-201756
Providing secure gateway between private and outside networks - disabling communications packet forwarding at gateway and processing any packet with matching network encapsulation address
Patent Assignee: MILKYWAY NETWORKS CORP (MILK-N)
Inventor: VU H T
Number of Countries: 006 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 713311	A1	19960522	EP 95308261	A	19951117	199625	B
CA 2136150	A	19960519	CA 2136150	A	19941118	199638	
US 5623601	A	19970422	US 94342772	A	19941121	199722	N

Priority Applications (No Type Date): CA 2136150 A 19941118; US 94342772 A 19941121
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 713311	A1	E	66		
Designated States (Regional): DE FR GB IT					
US 5623601	A		18		

Providing secure gateway between private and outside networks - ...

...**disabling communications packet forwarding at gateway and processing any packet with matching network encapsulation address**

...Abstract (Basic): be defined for given day, thereby improving security. Flexible. Assigns port numbers in real time. **Detects intrusion** attempts...
...Abstract (Equivalent): A method of providing a secure gateway between a private **network** and a potentially hostile **network**, comprising the steps of...

...a) addressing communications packets directly to a host on the potentially hostile **network** as if there were a communications path to the host, but encapulating the packets with...

...b) accepting at the gateway communications packets from either **network** that are encapsulated with a hardware destination address which matches the device address of the...
...Title Terms: **NETWORK;**

International Patent Class (Main): **G06F-011/00**...
International Patent Class (Additional): **G06F-012/14**
Manual Codes (EPI/S-X): **T01-H07C**...

...**T01-J12C**...

...**T01-S**

US005623601A

United States Patent [19]

Vu

[11] Patent Number: 5,623,601

[45] Date of Patent: Apr. 22, 1997

[54] APPARATUS AND METHOD FOR PROVIDING A SECURE GATEWAY FOR COMMUNICATION AND DATA EXCHANGES BETWEEN NETWORKS

[75] Inventor: Hung T. Vu, Ottawa, Canada

[73] Assignee: Milkway Networks Corporation, Ottawa, Canada

[21] Appl. No.: 342,772

[22] Filed: Nov. 21, 1994

[51] Int. Cl.[6] G06F 11/00

[52] U.S. Cl. 395/187.01; 395/188.01

[58] Field of Search 395/187.01, 188.01, 395/186, 182.02, 187.02, 180; 380/4

[56] References Cited

U.S. PATENT DOCUMENTS

5,023,907	6/1991	Johnson et al.	380/4
5,416,842	5/1995	Aziz et al.	380/4
5,548,646	8/1996	Aziz et al.	380/23

OTHER PUBLICATIONS

Stempel, "Ipaccess–an Internet Service Access System for Firewall Installations", Network and Distributed System Security, IEEE, pp. 31–41. Feb. 1995.

Nueman, "Proxy–Based Authproization and Accounting for Dsitributed Systems", Distributed Computing systems, IEEE Conf. pp. 283–291. Jan. 1993.

Bellovin et al., "Network Firewalls", IEEE Communications Magazinc. pp. 50–57 Sep. 1994.

Tirenin et al., "Enhanced Multinet Gateway: Survivable Multi–Level Secure Data Communications", Milcom IEEE, pp. 740–744 1991.

A Network Firewall, Marcus J. Ranum, Digital Equipment Corporation, Washington Open Systems Resource Center, Greenbelt, MD, Jun. 12, 1992.

White Paper–InterLock™ 2.1, Ans Co+Re Systems, Inc., Aug. 18, 1993.

Checkpoint Firewall–1™–Technical White Paper, Check-Point Software Technologies Ltd., 1994.

Thinking about Firewalls, Marcus J. Ranum, Trusted Information Systems, Inc. Glenwood, Md, 1993.

Socks, David Koblas and Michelle Koblas, 1993.

Internet Firewalls – An Overview, Marcus J. Ranum, A slide presentation, 1993, Trusted Information Systems, Inc.

Screen External Access Link (SEAL) Introductory Guide, Digital, publication date unknown.

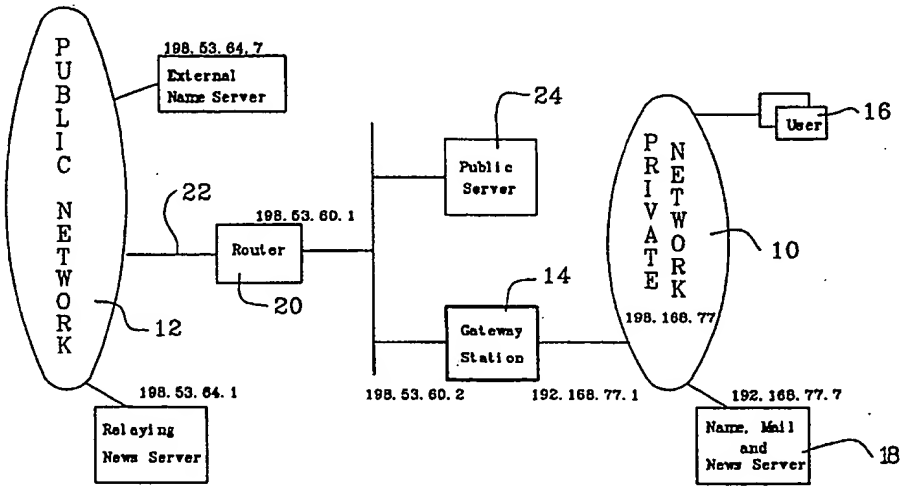
Increasing Security on IP Networks, Cisco Systems, Inc., advertising brochure, publication date unknown.

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Joseph E. Palys
Attorney, Agent, or Firm—Ralph H. Dougherty

[57] ABSTRACT

An apparatus and method for providing a secure firewall between a private network and a public network are disclosed. The apparatus is a gateway station having an operating system that is modified to disable communications packet forwarding, and further modified to process any communications packet having a network encapsulation address which matches the device address of the gateway station. The method includes enabling the gateway station to transparently initiate a first communications session with a client on a first network requesting a network service from a host on a second network, and a second independent communications session with the network host to which the client request was addressed. The data portion of communications packets from the first session are passed to the second session, and vice versa, by application level proxies which are passed the communications packets by the modified operating system. Data sensitivity screening is preferably performed on the data to ensure security. Only communications enabled by a security administrator are permitted. The advantage is a transparent firewall with application level security and data screening capability.

41 Claims, 7 Drawing Sheets



Gopher session. To enable transparent mode using the Telnet program, a Telnet session is started with gateway station 14 as follows:

your-host % telnet gatewaystation.company.com
Trying 198.53.64.2
Connected to gatewaystation.company.com
Escape character is '^]'
gatewaystation proxy-telnet ready:
Username: You
Password: xxxxxxx
Login Accepted
proxy-telnet>enable
proxy-telnet>quit
Disconnecting . . .
Connection closed by foreign host.
your-host %

A user may also authenticate and enable transparent mode using the FTP program as follows:

your-host % FTP gatewaystation.company.com
Connected to gatewaystation.company.com
220 gatewaystation proxy-FTP ready:
Name (gatewaystation.company.com:you): You
331 Enter authentication password for you
Password: xxxxxxx
230 User authentication to proxy
ftp>quote enable
Transparent mode enabled
ftp>quit
your-host%

In the preferred embodiment of the invention, a proprietary Gopher proxy is enabled to automatically initiate transparent mode after the user has successfully authenticated to the gateway station 14 by entering a valid user identification and password, whenever a Gopher session is requested and user authentication is required. This user authentication capability is a novel feature for a Gopher proxy. The proprietary source code for the novel Gopher proxy is appended hereto as Appendix C.

The modes for implementing transparent mode are, of course, arbitrary and may be redesigned or reassigned to other programs or proxies as those skilled in the art deem appropriate. Once the transparent mode is enabled, an authentication directory is updated by creating a file entry for the source IP address 32. The authentication files include a creation time variable which is automatically set to the system time when the file is created. This creation time variable is used to track the time of authentication. The files also include a last modification time variable which is automatically updated by the system each time the file is modified. By rewriting the authentication file each time a user initiates a new communications session through the gateway station 14 the time of last use of the gateway station can be tracked. This authentication directory is inspected periodically and user files are deleted from the authentication directory base on any number of predetermined criteria. In accordance with the preferred embodiment, the user file is deleted from the authentication directory if the user has not initiated a communications session through the gateway station for a period of time predefined by the systems administrator. In addition, the user file may be deleted from the authentication directory at a predetermined time of day defined by the system administrator. It is therefore possible to have the authentication of all users of the gateway station 14 revoked at a specified time of day, such as the end of the business day. This further fortifies the security of the gateway.

It is apparent that a novel and particularly invulnerable gateway has been invented. The gateway is efficient as well as secure. It will be readily apparent to those skilled in the art that modification may be made to the preferred embodiment described above without departing from the scope of the invention as expressed in the appended claims.

I claim:

1. A method of providing a secure gateway between a private network and a potentially hostile network, comprising the steps of:

(a) addressing communications packets directly to a host on the potentially hostile network as if there were a communications path to the host, but encapulating the packets with a hardware destination address that matches a device address of the gateway;

(b) accepting at the gateway communications packets from either network that are encapsulated with a hardware destination address which matches the device address of the gateway;

(c) determining at the gateway whether there is a process bound to a destination port number of an accepted communications packet;

(d) establishing transparently at the gateway a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the destination port number, else dropping the packet;

(e) establishing transparently at the gateway a second communications session with a destination address/destination port of the accepted communications packet if a first communications session is established; and

(f) transparently moving data associated with each subsequent communications packet between the respective first and second communications sessions, whereby the first session communicates with the source and the second session communicates with the destination using the data moved between the first and second sessions.

2. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the step of determining involves checking to determine if a process is bound to the destination port number, and passing the packet to a generic process if a process is not bound to the destination port number, the generic process acting to establish the first and second communications sessions and to move the data between the first and second communications sessions.

3. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the method further involves the steps of:

a) checking a rule base to determine if the source address requires authentication; and

b) authenticating the source by requesting a user identification and a password and referencing a database to determine if the user identification and password are valid.

4. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 1 wherein the method further involves the steps of:

a) referencing a rule base after the first communications session is established to determine whether the source address is permitted access to the destination address for a requested type of service; and

b) cancelling the first communications session if the rule base does not include a rule to permit the source address to access the destination address for the requested type of service.

5. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 3, wherein the method further involves the steps of:

a) creating a user authentication file which contains the source address of the authenticated user in a user authentication directory; and

b) referring to the authentication file to determine if a source address has been authenticated each time a new communications session is initiated so that the gateway is completely transparent to an authenticated source.

6. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 5 wherein the user authentication file includes a creation time variable which is set to a system time value when the user is authenticated.

7. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 6 wherein the method further involves the steps of:

a) updating a modification time variable of the authentication file each time the user initiates a new communications session through the gateway station.

8. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 7 wherein the method further involves the steps of:

a) periodically checking each user authentication file to determine whether one of a first difference between the authentication time variable and the system time and a second difference between the modification time variable and the system time has exceeded a predefined threshold; and

b) deleting the user file from the user authentication directory if the threshold has been exceeded by each of the first and second differences.

9. A method for providing a secure gateway between a private network and potentially hostile network as claimed in claim 1 wherein the method further involves the steps of:

a) performing a data sensitivity check on the data associated with each packet as a step in the process of moving the data between the respective first and second communications sessions.

10. A method of providing a secure gateway between a private network and a potentially hostile network, comprising the steps of:

(a) addressing communications packets directly to a host on the potentially hostile network as if there were a communications path to host, but encapulating the packets with a hardware destination address that matches a device address of the gateway;

(b) accepting from either network all TCP/IP packets that are encapsulated with a hardware destination address which matches the device address of the gateway;

(c) determining whether there is a proxy process bound to a port for serving a destination port number of an accepted TCP/IP packet;

(d) establishing a first communications session with a source address/source port number of the accepted TCP/IP packet if there is proxy process bound to the port for serving the destination port number, else dropping the packet;

(e) determining if the source address/source port number of the accepted packet is permitted to communicate with a destination address/destination port number of the accepted packet by referencing a rule base, and dropping the packet if a permission rule cannot be located;

(f) establishing a second communications session with the destination address/destination port number of the accepted TCP/IP packet if a first communications session is established and the permission rule is located; and

(g) transparently moving data associated with each subsequent TCP/IP packet between the respective first and second communications sessions, whereby the first session communicates with the source and the second session communicates with the destination using the data moved between the first and second sessions.

11. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 10 wherein the step of determining involves checking a table to determine if a custom proxy process is bound to the destination port number, and passing the packet to a generic proxy process if a custom proxy process is not bound to the destination port number, the generic proxy process being executed to establish the first and second communications sessions and to move the data between the first and second communications sessions.

12. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 10 wherein the step of establishing a first communications session with a source address/source port number further involves the steps of:

a) checking a rule base to determine if the source requires authentication;

b) checking an authentication directory to determine if an authentication file exists for the source in an instance where the source requires authentication; and

c) if the source requires authentication and an authentication file for the source cannot be located, authenticating the source by requesting a user identification and a password and referencing a user identification database to determine if the user identification and password are valid.

13. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 12 wherein the method further involves the steps of:

a) referencing a rule base as a first step after the first communications session is established to determine whether the user identification/password at the source address is permitted to communicate with the destination address for a requested service; and

b) cancelling the first communications session if the rule base does not include a rule to permit the user identification/password at the source address to communicate with the destination address for the requested type of service.

14. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 12, wherein the method further involves the steps of:

a) creating a user authentication file which contains the source address of the authenticated user in a user authentication directory; and

b) referring to the authentication file to determine if a source address has been authenticated each time a new communications session is initiated so that the gateway is completely transparent to an authenticated source having an authentication file in the authentication directory.

15. A method of providing a secure gateway between a private network and a potentially hostile network as claimed

in claim 14 wherein a file creation time variable which is automatically set by an operating system of the gateway station to a system time value when a file is created, is used to monitor a time when the user is authenticated.

16. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 14 wherein the method further involves the steps of:

a) rewriting the user authentication file each time the user initiates a new communications session through the gateway station so that a modification time variable in the authentication file is automatically updated by the operating system of the secure gateway.

17. A method of providing a secure gateway between a private network and a potentially hostile network as claimed in claim 16 wherein the method further involves the steps of:

a) periodically checking each user authentication file to determine whether one of a first difference between the authentication time variable and the system time and a second difference between the modification time variable and the system time has exceeded a predefined threshold; and

b) deleting the user file from the user authentication directory if the threshold has been exceeded by both of the first and second differences.

18. A method for providing a secure gateway between a private network and potentially hostile network as claimed in claim 10 wherein the method further involves the steps of:

a) performing a data sensitivity check on the data portion of each packet as a step in the process of moving the data between the respective first and second communications sessions, whereby the TCP/IP packet is passed by a modified kernel of an operating system of the secure gateway to the proxy process which extracts the data from the packet and passes the data from a one of the first and second communications sessions to a proxy process which operates at an application layer of the gateway station and the proxy process executes data screening algorithms to screen the data for elements that could represent a potential security breach before the data is passed to the other of the first and second communications sessions.

19. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network, comprising in combination:

a gateway station adapted for connection to a telecommunications connection with each of the private network and the potentially hostile network;

an operating system executable by the gateway station, a kernel of the operating system having been modified so that the operating system:

a) cannot forward any communications packet from the private network to the potentially hostile network or from the potentially hostile network to the private network; and

b) will accept for processing any communications packet from either of the private network and the potentially hostile network provided that the packet is encapsulated with a hardware destination address that matches the device address of the gateway station on the respective network; and

at least one proxy process executable by the gateway station, the at least one proxy process being adapted to transparently initiate a first communications session with a source of an initial data packet accepted by the operating system and to transparently initiate a second communications session with a destination of the packet without intervention by the source, and to transparently pass the data portion of packets received by the first communications session to the second communications session and to pass the data portion of packets received by the second communications session to the first communications session, whereby the first session communicates with the source using data from the second session and the second session communicates with the destination using data received from the first session.

20. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19 wherein the operating system is a Unix operating system.

21. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19 wherein the at least one proxy process includes modified public domain proxy processes for servicing Telnet, FTP, and UDP communications.

22. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19 wherein the at least one proxy process is a generic proxy process capable of servicing any network service which may be communicated within TCP/IP protocol, on any one of the 64K TCP/IP communications ports.

23. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 22 wherein the kernel is modified so that it will pass to the generic proxy process any communications packet having a destination port number that indicates a port to which no custom proxy process is bound, if the generic proxy process is bound to a predefined communications port when the communications packet is received by the kernel.

24. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 20 wherein the gateway station is a Unix station.

25. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19 wherein the apparatus further includes programs for providing a security administrator with an interface to permit the security administrator to build a rule base for controlling communications through the gateway station.

26. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19 wherein the at least one proxy process includes domain proxy processes for servicing Gopher and TCP communications.

27. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 19 wherein the Gopher proxy process is enabled to authenticate users whenever a Gopher session is initiated and user authentication is required.

28. Apparatus for providing a secure gateway for data exchanges between a private network and a potentially hostile network as claimed in claim 22 wherein the generic proxy process capable of servicing any network service which may be communicated within TCP/IP protocol, on any one of the 64K TCP/IP communications ports is a TCP proxy process.

29. A computer system for providing a secure gateway between a private network and a potentially hostile network, comprising:

a) means for accepting from either network all communications packets that are encapsulated with a hardware destination address which matches the device address of the gateway;

b) means for determining whether there is a process bound to a destination port number of an accepted communications packet;

c) means for establishing a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the destination port number, else dropping the packet;

d) means for transparently establishing, without intervention from the source, a second communications session with a destination address/destination port of the accepted communications packet if a first communications session is established; and

e) means for transparently moving data associated with each subsequent communications packet between the respective first and second communications sessions, whereby the first session communicates with the source and the second session communicates with the destination using the data moved between the first and second sessions.

30. A computer system providing a secure gateway between a private network and a potentially hostile network as claimed in claim **29** wherein the means for determining checks to determine if a process is bound to the destination port number, and passes the packet to a generic process if a process is not bound to the destination port number, the generic process acting to establish the first and second communications sessions and to move the data between the first and second communications sessions.

31. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim **29** wherein the system further includes:

a) means for checking a rule base to determine if the source address requires authentication; and

b) means for authenticating the source by requesting a user identification and a password and referencing a database to determine if the user identification and password are valid.

32. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim **29** wherein the system further includes:

a) means for referencing a rule base after the first communications session is established to determine whether the source address is permitted to access the destination address for a requested type of service; and

b) means for cancelling the first communications session if the rule base does not include a rule to permit the source address to access the destination address for the requested type of service.

33. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim **32**, wherein the system further includes:

a) means for creating a user authentication file which contains the source address of the authenticated user in a user authentication directory; and

b) means for referring to the authentication file to determine if a source address has been authenticated each time a new communications session is initiated so that the gateway is completely transparent to an authenticated source.

34. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim **33** wherein the user authentication file includes a creation time variable which is set to a system time value when the user is authenticated.

35. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim **34** wherein the system further includes:

a) means for updating a modification time variable of the authentication file each time the user initiates a new communications session through the gateway station.

36. A computer system for providing a secure gateway between a private network and a potentially hostile network as claimed in claim **35** wherein the system further includes:

a) means for periodically checking each user authentication file to determine whether one of a first difference between the authentication time variable and the system time and a second difference between the modification time variable and the system time has exceeded a predefined threshold; and

b) means for deleting the user file from the user authentication directory if the threshold has been exceeded by each of the first and second differences.

37. A computer system for providing a secure gateway between a private network and potentially hostile network as claimed in claim **29** wherein the system further includes:

a) means for performing a data sensitivity check on the data associated with each packet as a step in the process of moving the data between the respective first and second communications sessions.

38. A computer-readable memory encoded with computer-readable instructions for providing a secure gateway between a private network and a potentially hostile network, comprising:

a) instructions for accepting from either network all communications packets that are encapsulated with a hardware destination address which matches the device address of the gateway;

b) instructions for determining whether there is a process bound to a destination port number of an accepted communications packet;

c) instructions for transparently establishing a first communications session with a source address/source port of the accepted communications packet if there is a process bound to the destination port number, else dropping the packet;

d) instructions for transparently establishing, without intervention from the source, a second communications session with a destination address/destination port of the accepted communications packet if a first communications session is established; and

e) instructions for transparently moving data associated with each subsequent communications packet between the respective first and second communications sessions, whereby the first session communicates with the source and the second session communicates with the destination using the data moved between the first and second sessions.

39. A computer readable memory as claimed in claim **38** wherein the computer readable memory comprises at least one compact disk.

40. A computer readable memory as claimed in claim **38** wherein the computer readable memory comprises at least one floppy diskette.

41. A computer readable memory as claimed in claim **38** wherein the computer readable memory comprises at least one hard disk drive.

* * * * *

40/3,K/4 (Item 4 from file: 350) **Links**
Derwent WPIX

012872700 **Image available**
WPI Acc No: 2000-044533/**200004**
XRPX Acc No: N00-034113

Data processor for microcomputer system - has address monitoring mechanism interruption handler which forcefully terminates DMA forwarding, when interruption is required by trigger condition setting circuit during direct memory access

Patent Assignee: HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 11306095	A	19991105	JP 98106525	A	19980416	200004	B

Priority Applications (No Type Date): JP 98106525 A 19980416
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 11306095	A		20	G06F-013/00	

... **has address monitoring mechanism interruption handler which forcefully terminates DMA forwarding, when interruption is required by trigger condition setting circuit during direct memory access**

...Abstract (Basic): in performing DMA forwarding and data access to the next address of a forwarding completion **address**, based on trigger condition set-up. An **address** monitoring mechanism **interruption** handler (145) forcefully **terminates** DMA **forwarding**, when an **interruption** is required by a trigger condition setting circuit (140...

...ADVANTAGE - **Detects abnormal** direct memory access data forwarding and performs immediate stoppage to prevent damaging the stored data...

International Patent Class (Main): **G06F-013/00**
International Patent Class (Additional): **G06F-013/28**
Manual Codes (EPI/S-X): **T01-C07C**...

...**T01-F02A1**...

...**T01-H01C2**...

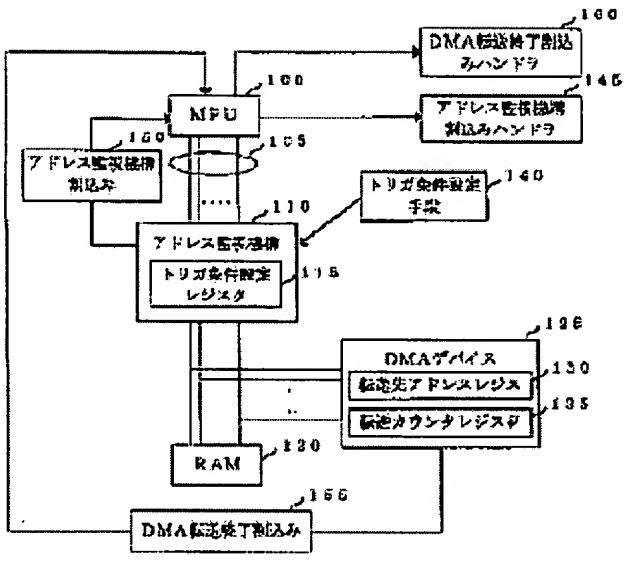
...**T01-H05B2**

DATA PROCESSOR

Publication number: JP11306095
Publication date: 1999-11-05
Inventor: OKAMOTO HIDEYUKI; TANAKA HIROYUKI; KIYONO TAKASHI; HAYASHI KAZUYA
Applicant: HITACHI LTD
Classification:
- international: ***G06F13/00; G06F13/28;*** **G06F13/00; G06F13/20;** (IPC1-7): G06F13/00; G06F13/28
- european:
Application number: JP19980106525 19980416
Priority number(s): JP19980106525 19980416

Abstract of **JP11306095**

PROBLEM TO BE SOLVED: To provide a data processor which detects abnormal DMA data transfer before the data are destructed by its execution, has the abnormal data transfer stopped and can avoid destruction of the data or system down. SOLUTION: A trigger condition set means 145 refers to a state flag which indicates whether an address monitoring mechanism 111 is transferring DMA or not and a DMA device 125 sets an address of a DMA transferred party + a transfer size +1 in a trigger condition set register 115. The DMA device 125 sets the state flag during transferring. When a trigger exception occurs during DMA transfer, an address monitoring mechanism interruption handler 145 forces DMA transfer to be completed, sets the state flag to be transfer completion and issues a signal. When a trigger condition set means 140 receives the signal, it refers to the state flag and clears the address monitoring mechanism 110.



```
Set     Items   Description
S1     208989   S ATTACK? OR ANOMAL? OR ABNORMAL?
S2     162269   S OVERFLOW? OR FLOOD? OR SYNFLOOD? OR VIRUS? OR WORM? ? OR TROJAN()HORSE?
OR MALWARE? OR MALICIOUS()CODE?
S3      23144   S DENIAL?(2W)SERVICE? OR INTRUSION? OR MALICIOUS? OR HOSTILE? OR
OVERWHELM? OR SWAMP?
S4     277722   S SUSPICIOUS? OR (ABNORM? OR ANOMAL?)(2N)ACTIVIT? OR HACK? OR PENETRAT? OR
ATTACK? OR VIOLAT? OR UNAUTHORI?
S5    2514425   S MONITOR? OR TRANSDUCE? OR TRANSDUCING? OR SENSING? OR DETECT? ? OR
DETECTION? OR DETECTED OR DETECTING
S6    1338414   S TRACK? OR AUDIT? OR POLL? OR INTERROGAT? OR PING? OR TEST? OR SURVEY?
S7    1688748   S SURVEILL? OR INSPECT? OR QUIZ? OR EVALUAT? OR ASSESS? OR ASCERTAIN? OR
MEASUR?
S8    1561527   S IDENTIF? OR DISCOVER? OR FIND? OR LOCAT? OR PINPOINT? OR SPOT? ? OR
SPOTTING? OR SPOTTED
S9     713229   S RECOGN? OR PERCEIV? OR DISCERN? OR EXPOSE? OR EXPOSING OR FERRET? OR
UNCOVER?
S10    119938   S S1:S4(10N)S5:S9
S11     27414   S INHIBIT? OR STOP? OR TERMINAT? OR END OR ENDS OR ENDED OR ENDING?
S12       629   S CEASE? OR CEASING OR CESSATION? OR ARREST? OR SHUT?()DOWN?
S13      1889   S SHUT?()DOWN? OR SHUTDOWN? OR DISABL? OR DISCONTINU? OR DEACTIVAT? OR
HALT?
S14      2552   S "NOT" ()ENABL? OR SUSPEND? OR SUSPENSION? OR CANCEL?
S15      6909   S AUTODISABL? OR NOGO OR NO()GO OR OFFSTATE? OR OFF()STATE? OR INTERRUPT?
OR TURNOFF? OR (TURN? OR SWITCH? OR SHUT?)()OFF
S16     25285   S ROUTE? OR ROUTING? OR SEND? OR BROADCAST? OR TRANSMIT? OR TRANSMISSION?
S17      8137   S FORWARD? OR DISEMINAT? OR DISSEMINAT? OR DISPATCH? OR FORWARD? OR
TRANSLOCAT? OR TRANSPORT?
S18      9042   S ADDRESS? OR RETURNADDRESS? OR LOCATION? OR LOCALE? OR LOCALIT? OR SITE?
? OR WEBADDRESS? OR URL OR URLADDRESS?
S19      5148   S REGION? ? OR SECTOR? ? OR MACADDRESS? OR IPADDRESS? OR NAT? ? OR
WEBSITE?
S20         7   S (WEB OR WORLD()WIDE()WEB OR ONLINE OR INTERNET OR LAN? ? OR WAN? ?)()(ID
OR IDENTIF? OR IDS)
S21     14474   S ROUTER? OR SWITCH?
S22       777   S (ROUTING OR SWITCHING)()(DEVICE? OR UNIT? OR APPARATUS? OR FIREWALL? OR
PROXY? OR SERVER?)
S23       402   S (ROUTING OR SWITCHING)()(UNIT? OR MODULE? OR COMPONENT? OR HARDWARE? OR
HUB? ? OR NODE?)
S24      5779   S NETWORK? OR LAN OR WAN OR LANS OR WANS OR ETHERNET? OR INTRANET? OR
EXTRANET? OR VPN? ?
S25      1648   S WEB OR (COMMUNICAT? OR TELECOM? OR TELCOM? OR TELNET?)()SYSTEM?
S26     13994   S IC=G06F?
S27     11858   S MC=T01?
S28     34594   S S10 AND S20:S27
S29        36   S S28 AND S11:S15(6N)S16:S17(6N)S18:S20
S30        66   S S10 AND S11:S15(5N)S16:S17(5N)S18:S20
S31        52   S S30 AND S1:S4(5N)S5:S9
S32        73   S S29:S31
S33        16   S S32 AND AC=US/PR
S34        13   S S33 AND AY=(1970:2000)/PR
S35        12   S S33 NOT AY=(2001:2006)/PR
S36        57   S S32 NOT S33
S37        37   S S36 AND PY=1970:2000
S38        36   S S36 NOT PY=2001:2006
S39        50   S S34:S35 OR S37:S38
S40        50   IDPAT (sorted in duplicate/non-duplicate order)
 ; show files
```

[File 347] **JAPIO** Dec 1976-2005/Dec(Updated 060404)

[File 350] **Derwent WPIX** 1963-2006/UD,UM &UP=200639

**File 350: Preview the enhanced DWPI through ONTAP DWPI (File 280). For more information, visit http://www.dialog.com/dwpi/.*

```
Set     Items   Description
S1    1359772   S ATTACK? OR ANOMAL? OR ABNORMAL?
S2     998419   S OVERFLOW? OR FLOOD? OR SYNFLOOD? OR VIRUS? OR WORM? ? OR TROJAN()HORSE?
OR MALWARE? OR MALICIOUS()CODE?
S3     136889   S DENIAL?(2W)SERVICE? OR INTRUSION? OR MALICIOUS? OR HOSTILE? OR
OVERWHELM? OR SWAMP?
S4     768086   S SUSPICIOUS? OR (ABNORM? OR ANOMAL?)(2N)ACTIVIT? OR HACK? OR PENETRAT? OR
ATTACK? OR VIOLAT? OR UNAUTHORI?
S5    4539501   S MONITOR? OR TRANSDUCE? OR TRANSDUCING? OR SENSING? OR DETECT? ? OR
DETECTION? OR DETECTED OR DETECTING
S6    9200986   S TRACK? OR AUDIT? OR POLL? OR INTERROGAT? OR PING? OR TEST? OR SURVEY?
S7   14086580   S SURVEILL? OR INSPECT? OR QUIZ? OR EVALUAT? OR ASSESS? OR ASCERTAIN? OR
MEASUR?
S8    7120641   S IDENTIF? OR DISCOVER? OR FIND? OR LOCAT? OR PINPOINT? OR SPOT? ? OR
SPOTTING? OR SPOTTED
S9    2084886   S RECOGN? OR PERCEIV? OR DISCERN? OR EXPOSE? OR EXPOSING OR FERRET? OR
UNCOVER?
S10    510971   S S1:S4(10N)S5:S9
S11     45424   S INHIBIT? OR STOP? OR TERMINAT? OR END OR ENDS OR ENDED OR ENDING?
S12      3452   S CEASE? OR CEASING OR CESSATION? OR ARREST? OR SHUT?()DOWN?
S13      5364   S SHUT?()DOWN? OR SHUTDOWN? OR DISABL? OR DISCONTINU? OR DEACTIVAT? OR
HALT?
S14      5023   S "NOT" ()ENABL? OR SUSPEND? OR SUSPENSION? OR CANCEL?
S15      1821   S AUTODISABL? OR NOGO OR NO()GO OR OFFSTATE? OR OFF()STATE? OR INTERRUPT?
OR TURNOFF? OR (TURN? OR SWITCH? OR SHUT?)()OFF
S16     40274   S ROUTE? OR ROUTING? OR SEND? OR BROADCAST? OR TRANSMIT? OR TRANSMISSION?
S17     27138   S FORWARD? OR DISEMINAT? OR DISSEMINAT? OR DISPATCH? OR FORWARD? OR
TRANSLOCAT? OR TRANSPORT?
S18     62125   S ADDRESS? OR RETURNADDRESS? OR LOCATION? OR LOCALE? OR LOCALIT? OR SITE?
? OR WEBADDRESS? OR URL OR URLADDRESS?
S19     53135   S REGION? ? OR SECTOR? ? OR MACADDRESS? OR IPADDRESS? OR NAT? ? OR
WEBSITE?
S20        22   S (WEB OR WORLD()WIDE()WEB OR ONLINE OR INTERNET OR LAN? ? OR WAN? ?)()(ID
OR IDENTIF? OR IDS)
S21      4311   S ROUTER? OR SWITCH?
S22        34   S (ROUTING OR SWITCHING)()(DEVICE? OR UNIT? OR APPARATUS? OR FIREWALL? OR
PROXY? OR SERVER?)
S23        21   S (ROUTING OR SWITCHING)()(UNIT? OR MODULE? OR COMPONENT? OR HARDWARE? OR
HUB? ? OR NODE?)
S24     23685   S NETWORK? OR LAN OR WAN OR LANS OR WANS OR ETHERNET? OR INTRANET? OR
EXTRANET? OR VPN? ?
S25      4321   S WEB OR (COMMUNICAT? OR TELECOM? OR TELCOM? OR TELNET?)()SYSTEM?
S26     28483   S S10 AND S1:S4(10N)S5:S9 AND S20:S25
S27         9   S S26 AND S11:S15(5N)S16:S17(5N)S18:S20
S28        31   S S11:S15(5N)S16:S17(5N)S18:S20 AND S10 AND S1:S4(5N)S5:S9
S29        32   S S27:S28
S30        13   S S29 AND PY=1970:2000
S31        13   S S29 NOT PY=2001:2006
S32        13   S S30:S31
S33        13   RD  (unique items)
 ; show files
```

[File 2] **INSPEC** 1898-2006/Jun W2

[File 6] **NTIS** 1964-2006/Jun W2

[File 8] **Ei Compendex(R)** 1970-2006/Jun W2

40/3,K/13 (Item 13 from file: 350) Links
Derwent WPIX

010646685 **Image available**
WPI Acc No: 1996-143639/**199615**
XRPX Acc No: N96-120414
Interrupt processing system for abnormal microcomputer operation - has occupancy monitoring circuit that detects undesired signal, interrupts CPU and sends halt notification signal suspending CPU access address space operation

Patent Assignee: HITACHI CHUBU SOFTWARE KK (HITA-N); HITACHI LTD (HITA)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 8030491	A	19960202	JP 94160940	A	19940713	199615	B

Priority Applications (No Type Date): JP 94160940 A 19940713
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 8030491	A		4	G06F-011/30	

... **has occupancy monitoring circuit that detects undesired signal, interrupts CPU and sends halt notification signal suspending CPU access address space operation**

...Abstract (Basic): The bus end signal loops back to the bus controller. The occupancy time **monitoring** circuit **detects** an undesired signal that causes **abnormality** to central processor operation which in turn **sends** a time out notification signal (1a) and **suspends** the access **address** space operation of the central processor...
International Patent Class (Main): **G06F-011/30**
International Patent Class (Additional): **G06F-013/00**...

...**G06F-013/36**
Manual Codes (EPI/S-X): **T01-G05C**...

...**T01-H05B3**

TIME-OUT PROCESSING SYSTEM

Publication number: JP8030491
Publication date: 1996-02-02
Inventor: IDE JUNYA; KARASAKI SADAJI; TERAO MASUMI; INAGAWA TAKASHI
Applicant: HITACHI LTD; HITACHI CHUBU SOFTWARE KK
Classification:
- international: ***G06F11/30; G06F13/00; G06F13/36;*** **G06F11/30; G06F13/00; G06F13/36;** (IPC1-7): G06F11/30; G06F11/30; G06F13/00; G06F13/36
- european:
Application number: JP19940160940 19940713
Priority number(s): JP19940160940 19940713

Abstract of **JP8030491**

PURPOSE:To improve RAS by abnormality processing by a time-out on a new system bus by making an address, which causes the time-out of a system bus, distinctive between a mounted space and an unmounted space by a microprogram and performing the abnormality processing. CONSTITUTION:To discriminate whether the time-out reported to a central processor 11 is a time-out due to a fault of an IO in the mounted space or a time-out originating from actuation to the unmounted space, the microprogram discriminates whether the address at the time of the time-out occurrence is in the mounted space. When the address is in the unmounted space, the abnormality processing is not performed similarly to software which supports a nonresponse type bus 16 to make the software compatible. When the address is in the mounted space, on the other hand, the abnormality processing is performed to know the fault etc., of a response type system bus 14FI/0 with a time-out report signal, thereby improving the RAS.